



RA Jan Möller

SPIT-AL
Rechtskonforme Abwehr
von SPAM over Internet Telephony (SPIT)

Das ULD-i



Was ist das ULD-i?

- Innovationszentrum Datenschutz und Datensicherheit beim ULD
- Ziel: Entwicklung und Durchführung von Projekten zur datenschutzkonformen und datenschutzfreundlichen Technikgestaltung
- Projektpartner aus dem öffentlichen und privaten Bereich

Referent

- Tätigkeit als Jurist für die Datenschutzaufsichtsbehörde Referat „Privacy-Enhancing Technologies“
- Aktuelle Projekte:
 - PRIME (Privacy and Identity Management for Europe)
 - PRISE (Entwicklungsleitlinien zum Datenschutz für die europäische Sicherheitsforschung)
 - SPIT-AL (SPAM over Internet Telephony-Abwehr-Lösung)

Das Projekt SPIT-AL

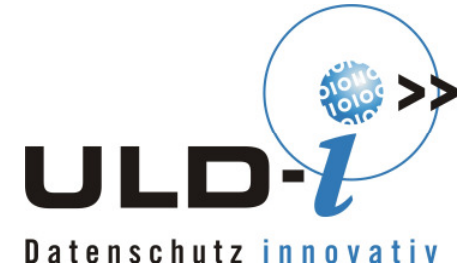
- Rahmenbedingungen
- Motivation
- Projektziele
- Eckpunkte der Entwicklung
- Rechtliche Gestaltungsvorgaben
- Technische Ansätze

Grundlegende Datenschutzfragen im Rahmen des Projektes

- Teilnehmerkennung
- Transportsicherheit
- Nutzerzentriertes Identitätsmanagement
- Reputationssysteme

Das Projekt SPIT-AL

Rahmenbedingungen



Die Projektpartner

- Projekt der TNG – The Net Generation AG in Kiel (Internet- und Telekommunikationsprovider) mit Unterstützung des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (durch das ULD-i)

Förderung

- Öffentliche Förderung 2005 – 2006:
e-Region Plus (Schleswig-Holstein)
EFRE – Europäischer Fonds für Regionale Entwicklung

Das Projekt SPIT-AL

Motivation



Das Problem

- Auftreten von **SPIT ist wirtschaftlich wahrscheinlich**: VoIP wird sich für Telefonie stark kostensenkend auswirken ⇒ Attraktivität als Werbe- und Kontaktmedium zu gewerblichen Zwecken steigt (E-Mail-Effekt)
- SPAM ⇒ **SPIT**, z.B. automatisierte Cold Calls sind **für die Privatsphäre noch unangenehmer**, da synchrones Medium
- E-Mail zeigt **technische und rechtliche Grenzen der SPAM-Bekämpfung** auf

Lösungsansätze

- Vermeidung von nicht durchdachten Lösungen durch **frühzeitige Beschäftigung** mit der Problematik
- Steuerung durch **kostenlose Bereitstellung** rechtskonformer (**Privacy by Design**) Lösung
- Stärkung von Betroffenenrechten durch **Rechtssicherheit** für Anwender von Beginn an

Das Projekt SPIT-AL

Projektziele



Konzeption und Entwicklung

- Rechtskonformer Filter für die Internet-Telefonie (ULD, TNG)

Technische Umsetzung

- Implementierung eines Prototyps (TNG, Diplomarbeit TU Dresden)

Praxistest

- Probebetrieb und Evaluation (TNG, ULD)

Das Projekt SPIT-AL

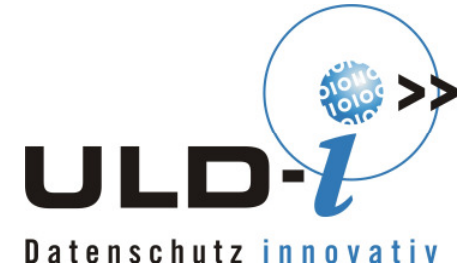
Eckpunkte der Entwicklung



- Grundkonzeption abgeschlossen, White Paper ist veröffentlicht:
<http://www.spit-abwehr.de>
(Feedback erwünscht!)
- Diverse Gestaltungsoptionen offen, Details auf dem VoIP Security-Workshop im Juni in Berlin
- Diplomarbeit (TU Dresden)
- Prototyp in Entwicklung (teilweise auf Asterisk-Basis)
- Probebetrieb mit 1.000 Nutzern bis Ende 2006
- Open Source-Projekt
- Integration weiterer Dienste, z.B. medienübergreifendes Erreichbarkeits- und Identitätsmanagement

Das Projekt SPIT-AL

Rechtliche Gestaltungsvorgaben I



Fernmeldegeheimnis

- Art. 10 GG, § 88 TKG, § 206 StGB
- Schützt Inhalt der Kommunikation und die Tatsache, dass diese überhaupt stattgefunden hat (auch erfolglose Verbindungsversuche).
- Verpflichtet Telekommunikationsanbieter und deren Mitarbeiter.
- ⇒ Kontrolle über SPIT-Filter muss in Hand des Nutzers (als Angerufener) liegen

Das Projekt SPIT-AL

Rechtliche Gestaltungsvorgaben II



Telekommunikationsrecht

- § 88 Fernmeldegeheimnis
- Überwachungsmaßnahmen für Bedarfsträger: Übergangslösung bis Ende 2007
- TK-rechtlich ist VoIP noch wenig erschlossen
 - Eckpunktepapier der Bundesnetzagentur
 - EU Commission Staff Working Document: The Treatment of Voice over Internet Protocol (VoIP) under the EU Regulatory Framework
- Technik oder Dienst?

Das Projekt SPIT-AL

Rechtliche Gestaltungsvorgaben III



Datenschutzrecht

- §§ 91 - 107 TKG, Umfeld: TDDSG, BDSG
- SPIT-Filter als Auftragsdatenverarbeitung?
- Unterschiedliche SPIT-AL-Maßnahmen für Privatpersonen, Unternehmen oder Behörden (Verwaltungsrecht: Gewährung rechtlichen Gehörs)
- Whitelists / Blacklists bedeuten Verarbeitung personenbezogener Daten ⇒ Infrastruktur für Einwilligung / Widerruf ⇒ Telediensterecht
- SPAM-Filterung als erforderliche TO-Maßnahme (als Massenphänomen / Einzelbetrachtung)

Das Projekt SPIT-AL

Rechtliche Gestaltungsvorgaben IV



Aufforderung an Hersteller, Anbieter und Anwender von VoIP-Lösungen (Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Oktober 2005)

- Grundgesetzlich geschütztes Fernmeldegeheimnis bewahren!
- Angemessene technische und organisatorische Maßnahmen treffen, um sichere und datenschutzgerechte Nutzung von VoIP in einem Netzwerk zu ermöglichen.
- Verschlüsselungsverfahren anbieten bzw. nutzen. Sicherheits- und Datenschutzängel in Protokollen und Software durch Beteiligung an Weiterentwicklung möglichst schnell beseitigen.
- Offene und standardisierte Lösungen verwenden, Protokolle offenlegen. VoIP-Kunden über Gefahren und Einschränkungen gegenüber PSTN informieren.
- Bei VoIP alle datenschutzrechtlichen Vorschriften genauso wie bei herkömmlicher Telefonie beachten.

Das Projekt SPIT-AL

Rechtliche Gestaltungsvorgaben V



Working Paper zur SPAM-Filterung der Art. 29 Working Group

Abgeleitete Anforderungen an die Gestaltung der SPIT-AL:

- Nutzerkontrolle der Filterung
- Transparenz der Datenverarbeitung
und ihrer Folgen
- Einstelloptionen feingranular
- Voreinstellungen für verschiedene Nutzergruppen
(Privatnutzer, Unternehmen, öffentliche Stellen)

Das Projekt SPIT-AL

Technische Ansätze I

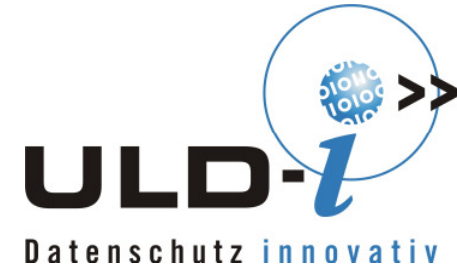


Erhebung und Auswertung von Informationen über Anrufer

- Anruferkennung? (P: Fehlende Authenticity bei SIP)
- Herkunft: PSTN / SIP (Proxy, IP-Range)?
- Whitelists / Buddylists / Blacklists
- Rekursive Listen / Vertrauensnetz (Distributed Whitelists)
- Statistische Verfahren

Das Projekt SPIT-AL

Technische Ansätze II



Auswertung des Kommunikationsinhaltes

- Geht nicht vor Anruf, da synchrones Medium
- Technisch sehr aufwändig
- Möglicherweise Eingriff in Fernmeldegeheimnis
- In SPIT-AL **nicht** vorgesehen

Das Projekt SPIT-AL

Technische Ansätze III



Verschiedene Maßnahmen als Reaktion auf Anruferauswertung

- Durchleiten zum Angerufenen
- „Besetzt“ beim ersten Versuch (Greylisting)
- Aufgabe für den Anrufer: „*Bitte drücken Sie #42#.*“ (Voice-Menü, gegen Automated Calling Machines)
- Durchleiten zum Anrufbeantworter für asynchrone Übermittlung
- Hinweis auf alternativen Gesprächsaufbau (Festnetz, kostenpflichtig als Initialkontakt)
- Ablehnen des Anrufes (P: Nachrichtenunterdrückung)

Grundlegende Datenschutzfragen im Rahmen des Projektes



Teilnehmererkennung

- Problem: Sichere Teilnehmerauthentifizierung (Einfache Veränderungsmöglichkeit der Teilnehmerkennungen)
- Z.B.: Mailbox-Authentifizierung über Teilnehmerkennung
- Z.B.: Mehrwertdienste auf Kosten Dritter nutzen

Grundlegende Datenschutzfragen im Rahmen des Projektes



Transportsicherheit

- SIP / RTPSecurity: Broken by Design?
- zfone von Phil Zimmermann
- SkypeSecurity: by Obscurity
Reverse Engineering: Skype Protokoll über Internet
Telephonie hinaus „nutzbar“

Grundlegende Datenschutzfragen im Rahmen des Projektes



Nutzerzentriertes Identitätsmanagement

- Effektive SPIT-Abwehr erfordert kontextbasiertes Call-Management
- Kontexterfassung und -auswertung beinhaltet (personenbezogene) Datenverarbeitung, die teilweise weitere Rückschlüsse auf soziale Netzwerke, Verhalten etc. ermöglicht
- Um Sekundärnutzungen zum Nachteil des Nutzers auszuschließen, ist die Einbindung in ein nutzerzentriertes Identitätsmanagement (⇒ <http://www.prime-project.eu/>) sinnvoll

Grundlegende Datenschutzfragen im Rahmen des Projektes



Reputationssysteme

- Synchrone Kommunikation ist nicht sinnvoll in Echtzeit auszuwerten ⇒ Erfahrungswerte aus der Vergangenheit werden eine Rolle spielen
- Erfahrungswerte (Reputation) können an verschiedenen (personenbezogenen) Daten ansetzen
- Reputation des Reputationsgebers ist wichtig, Rückverfolgung durch Betroffene zur Beseitigung von ungerechtfertigten Diskriminierungen soll möglich sein
⇒ soziale Netzwerke werden offenbar (anderweitige Missbrauchsmöglichkeit eröffnet)
- Beispiel: Distributed Whitelists



Datenschutz innovativ

Mit uns können Sie's machen.

Weitere Informationen unter
<http://www.uld-i.de/>

Abruf dieser Folien unter
<http://www.spit-abwehr.de/>

RA Jan Möller

LD103@datenschutzzentrum.de